

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年12月11日

出 願 番 号

Application Number:

特願2002-359072

[ST.10/C]:

[JP 2002-359072]

出 願 人

Applicant(s):

松下電器産業株式会社

2003年 6月20日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3048723

【書類名】 特許願

【整理番号】 2032740164

【提出日】 平成14年12月11日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 庄田 幸恵

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 廣田 照人

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 井藤 好克

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 暗号化データ復号装置、および暗号化データ復号方法

【特許請求の範囲】

【請求項 1】 単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、

前記プログラムの記憶装置上の位置情報を保持するアドレステーブル情報保持部と、

暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号部と、

前記暗号鍵を保持する暗号鍵保持部と、

前記暗号化データ復号部に復号指示を出し、前記アドレステーブル情報保持部が保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号して、前記メモリ配置情報保持部が保持するメモリ空間上の配置位置にロードする制御部と、

を有することを特徴とする暗号化データ復号装置。

【請求項 2】 分割され暗号化されたプログラムをメモリ空間にコピーし、ロードした位置、ロードした分割プログラムのサイズ、プログラム識別子をアドレステーブル情報保持部に記憶させると同時に、ロードしたアドレスにすでに他の分割プログラムがロードされていた場合にはその分割プログラムの管理情報をアドレステーブル情報保持部から削除するプログラム配置位置決定部をさらに有することを特徴とする請求項 1 記載の暗号化データ復号装置。

【請求項 3】 分割され暗号化されたプログラムをロードするためのメモリ空間の開始位置とそのサイズを指定するプログラムロード領域指定部をさらに有することを特徴とする請求項 1 記載の暗号化データ復号装置。

【請求項 4】 単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持ステップと、

前記プログラムの記憶装置上の位置情報を保持するアドレステーブル情報保持ステップと、

暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号ステップと、

前記暗号鍵を保持する暗号鍵保持ステップと、

前記暗号化データ復号部に復号指示を出し、前記アドレステーブル情報保持ステップが保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号して、前記メモリ配置情報保持ステップが保持するメモリ空間上の配置位置にロードする制御ステップと、

を包含することを特徴とする暗号化データ復号方法。

【請求項 5】 分割され暗号化されたプログラムをメモリ空間にコピーし、ロードした位置、ロードした分割プログラムのサイズ、プログラム識別子をアドレステーブル情報保持ステップに記憶させると同時に、ロードしたアドレスにすでに他の分割プログラムがロードされていた場合にはその分割プログラムの管理情報をアドレステーブル情報保持ステップから削除するプログラム配置位置決定ステップをさらに包含することを特徴とする請求項 4 記載の暗号化データ復号方法。

【請求項 6】 分割され暗号化されたプログラムをロードするためのメモリ空間の開始位置とそのサイズを指定するプログラムロード領域指定ステップをさらに包含することを特徴とする請求項 4 記載の暗号化データ復号方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、実行プログラムの逆解析や不正使用を防止する暗号化データ復号装置および暗号化データ復号方法に関する。

【 0 0 0 2 】

【従来の技術】

従来、暗号方式をコンピュータシステムに提供し、暗号化されたプログラムやデータを復号して利用する場合には、そのシステムの上で動作する復号プログラムを実行する。このとき、仕様が公開されたオープンなコンピュータシステムに置いては、プログラムの解析および改変が容易であるため、復号プログラムを改変することにより、もとの復号プログラムの仕様に反して、復号したデータを不正に利用することが簡単にできてしまい、システム全体の安全性は低くなるとい

う問題があった。

【 0 0 0 3 】

この問題を解決しようとする提案として、復号プログラム自体を暗号化し、データ復号時にのみ復号プログラムを復号して、データ復号作業を行う手段を採用し、これにより、復号プログラムの解析および改竄を困難にするものが知られている（例えば、特許文献 1 参照）。しかし、復号プログラムを復号するプログラムの解析、および改竄が成功すると、改竄プログラムの実行を防ぐことはできない。これに対し、復号プログラムの正当性を暗号化データの復号時に認証できるようにし、改竄された復号プログラムによる意図しない目的への復号したデータの流用を防止する提案がある（例えば、特許文献 2 参照）。

【 0 0 0 4 】

ところが、正当性が証明された復号プログラムを実行する場合には、コンピュータシステム上のメモリに復号された状態でプログラムがロードされる。このときに、不正な割り込み等により処理の流れを横取りされると、全てのプログラムが覗き見されてしまう。

【 0 0 0 5 】

また、メモリ上へのプログラムのロード方法として、オーバレイリンカ／ローダが知られている（例えば、非特許文献 1 参照）。オーバレイは、プログラムサイズよりも小さいメモリにプログラムを収めるために使われる手法である。プログラムのコードを小さなサイズでセグメント分割する。オーバレイのいくつかのセグメントは、同じメモリを共有する。プログラムが起動するとき、システムは、プログラムのエントリポイントを持つセグメントをロードする。オーバレイローダは、呼び出し先へのパスが含まれる各セグメントを、必要に応じて随時、ロードする。

【 0 0 0 6 】

しかし、従来のオーバレイリンカ／ローダでは、必要なセグメントを必要な時に順に限られた大きさのメモリ上にロードし、要らなくなったときに削除、または、他のプログラムが上書きすることによって消去されるため、メモリ上にプログラムのコードやデータが残されたままの状態になってしまうという問題があっ

た。また、オーバレイローダがプログラムをロードするアドレスが固定されるため、プログラムへのアクセスが容易に解読できてしまうという問題があった。

【0007】

以上のように、従来の技術では、一般的なコンピュータシステムにおいては、復号プログラムがメモリ上にロードされているときに不正な割り込みが発生した場合、全てのプログラムが覗き見されてしまい、復号プログラムのアルゴリズムや暗号鍵が暴露されてしまう。また、近年のコンピュータシステムは、メモリに制約を持たないのでオーバレイの手法を用いることはほとんどなく、プログラム全体をメモリ上に展開している。このため、システム全体の安全性が低くなってしまいう問題がある。

【0008】

【特許文献1】

特開平9-6232号公報

【特許文献2】

特開平11-39156号公報

【非特許文献1】

Linkers & Loaders, John R. Levine, オーム社、p165

【0009】

【発明が解決しようとする課題】

本発明は、仕様が公開されているオープンなコンピュータシステムにおいても、プログラムを部分的に復号しながらメモリ上にロードできるようにすることにより、不正な割り込み等で処理の流れが横取りされても、メモリ上からプログラムの全体の覗き見を防止することを目的としている。

【0010】

【課題を解決するための手段】

この課題を解決するために、本発明は、単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、前記プログラムの記憶装置上の位置情報を保持するアドレ

ステーブル情報保持部と、暗号化されたデータを暗号鍵に基づき復号する暗号化データ復号部と、前記暗号鍵を保持する暗号鍵保持部と、前記暗号化データ復号部に復号指示を出し、前記アドレステーブル情報保持部が保持する情報に従って前記プログラムを記憶装置上から読み出し、暗号化された前記プログラムを復号して前記メモリ配置情報保持部が保持するメモリ空間上の配置位置にロードする制御部とを備えたものである。

【 0 0 1 1 】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて説明する。

【 0 0 1 2 】

（実施の形態 1）

図 1 は、本発明の暗号化データ復号装置の構成を示す機能ブロック図である。図 1 においてメモリ配置情報保持部 1 0 4 は単位毎に分割されたプログラムを実行する際にメモリ空間上の配置位置を示す情報を保持し、アドレステーブル情報保持部 1 0 3 は、分割されたプログラムがメモリ上のどの位置に格納されているかという情報を暗号化して保持している。また暗号化データ復号部 1 0 2 は、暗号化されたデータを暗号鍵に基づき復号し、暗号鍵保持部 1 0 1 は暗号化データ復号部 1 0 2 が暗号化データを復号化する際に用いる暗号鍵を保持し、またアドレス情報認証部 1 0 5 は、アドレステーブル情報保持部 1 0 3 が保持する情報が正当なものか否かを認証し、メモリアドレス定義部 1 0 8 はメモリ配置情報保持部 1 0 4 の保持するメモリ空間上の配置位置をプログラム生成時にあらかじめ定義する。

【 0 0 1 3 】

プログラム生成部 1 1 1 はメモリアドレス定義部 1 0 8 が定義した情報に基づいて単位毎に分割され暗号化されたプログラムを生成する。暗号化情報復号部 1 0 9 は、暗号化されたメモリ配置情報保持部 1 0 4 の配置情報を暗号鍵に基づき復号する。暗号化テーブル情報復号部 1 1 0 は暗号化されたアドレステーブル情報保持部 1 0 3 の位置情報を暗号鍵に基づき復号する。不正アクセス防止部 1 0 7 は、プログラム実行中に割り込み等により不正に処理の流れを奪われた場合に

、それを検知し対抗措置をとる。さらに復号支援プログラム認証部100は暗号化データ復号部102が暗号化されたデータを復号する際に用いる復号支援プログラムが正当なものか否かを認証する。制御部106は、暗号化データ復号部102に復号指示を出し、アドレステーブル情報保持部103が保持する情報に従ってメモリ配置情報保持部104が保持するメモリ空間上の配置位置に従って単位毎にコンピュータシステムのメモリ空間上にプログラムを配置しながら実行する。

【0014】

図2は、制御部106が配置するメモリ配置構成の概念図である。

【0015】

図3は、メモリ配置情報保持部104が保持する暗号化されたアドレス情報および復号化されたアドレス情報およびハードディスク上のイメージ図である。

【0016】

図4は、メモリ配置情報保持部104が保持するメモリ空間上の配置位置を示す情報の概念図である。

【0017】

上記のような構成の暗号化データ復号装置において単位毎に分割されたプログラムのロード処理の具体的な流れを図5を用いて説明する。

【0018】

ここでいうプログラムのロードとは、プログラムを実行できるようにハードディスクのような2次記憶装置からメインメモリにコピーすることである。また単位毎に分割されたプログラムとは、1つのソースファイルまたは関連するソースファイルのグループから生成されたオブジェクトコードを指している。このオブジェクトコードとは具体的には一つのプログラムを構成する一部分を示すサブプログラムであったりあるいはライブラリモジュールそのものを指している。

【0019】

<プログラムのロード手順>

1. 制御部106は、暗号化テーブル情報復号部110に対してデータを復号化するよう指示を出し（S501）、続いてロードすべきプログラムAが格納さ

れているアドレスの情報を取得するためにアドレステーブル情報保持部103の情報を読み出す(S502)。

【0020】

2. 暗号化テーブル情報復号部110は、制御部106から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する(S503)。この認証処理に用いる情報の例として、プログラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【0021】

3. 2. で認証に成功した場合、暗号化テーブル情報復号部110は、図3の(3-1)に示すようなデータを暗号鍵保持部101が保持している暗号化されたデータを復号するための鍵に基づき読み出したデータを復号し(S504)、プログラムAが格納されている図3の(3-2)に示すようなアドレスの情報を得る。もし2. で認証に失敗した場合、暗号化テーブル情報復号部110はデータの復号を行わずプログラムの処理を中断し(S517)、制御部106は、メモリ空間上に復号されたデータがロードされている場合は消去する(S518)。

【0022】

4. 続いてアドレス情報認証部105は、3. で得たアドレス情報が正当なものであるか否かを認証する(S505)。この認証には、2. の認証処理で用いたものと同じ一方向ハッシュ関数等、一般に用いられている認証技術を用いる。アドレス情報認証部105がアドレス情報が正当なものであると認証した場合に、ステップ5. に進み、認証に失敗した場合は、制御部106はプログラムの処理を中断し(S517)、メモリ空間上にデータがロードされている場合は消去する(S518)。

【0023】

5. 引き続き制御部106は、暗号化データ復号部102に指示を出す(S506)。

【 0 0 2 4 】

6. 暗号化データ復号部 1 0 2 は、制御部 1 0 6 から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する（S 5 0 7）。この認証処理に用いる情報の例として、プログラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【 0 0 2 5 】

7. 6. で認証に成功した場合、図 3 の（3 - 3）に示すようなハードディスクの該当のアドレス位置から読み出したプログラム A を読み出す（S 5 0 8）。暗号化データ復号部 1 0 2 は読み出された暗号化されたプログラム A を復号する（S 5 0 9）。6. で認証に失敗した場合、データの復号を行わずプログラムの処理を中断し（S 5 1 7）、制御部 1 0 6 は、メモリ空間上に復号されたデータやプログラムがロードされている場合は消去する（S 5 1 8）。

【 0 0 2 6 】

8. さらに制御部 1 0 6 は、暗号化情報復号部 1 0 9 に復号指示を出す（S 5 1 0）。

【 0 0 2 7 】

9. 暗号化情報復号部 1 0 9 は、制御部 1 0 6 から復号指示を受け取ると、データを復号する際に実行する復号支援プログラムが正当なものであるか否かを認証する（S 5 1 1）。この認証処理に用いる情報の例として、プログラムのサイズ、更新日時、あるいはプログラムの一方向ハッシュ値を用いて元の復号支援プログラムが実行時に改ざんされていないかを認証する。もちろん、この認証手段は電子署名認証技術などの一般に公開されている技術を用いてもよい。

【 0 0 2 8 】

1 0. 9. で認証に成功した場合、暗号化情報復号部 1 0 9 はメモリ配置情報保持部 1 0 4 が保持する図 4 に示すようなメモリ空間上の配置位置情報の情報を読み出し（S 5 1 3）、読み出されたメモリ空間上の配置位置情報を復号化し（S 5 1 4）、復号化された配置位置情報に従ってプログラム A を予め定められた

メモリ空間上のOS 1-1というメモリ空間にロードする(S 5 1 5)。9. で認証に失敗した場合、配置情報の復号化は行わずに、プログラムの処理を中断し(S 5 1 7)、制御部 1 0 6 は、メモリ空間上に復号されたデータがロードされている場合は消去する(S 5 1 8)。

【 0 0 2 9 】

1 1. 制御部 1 0 6 は、プログラム A が呼び出す順に分割されたプログラム B ~ プログラム I を 1. ~ 1 0. の手順を繰り返すことによりロードする。

【 0 0 3 0 】

上記に述べたステップの暗号鍵保持部 1 0 1 は、具体的には例えばDESのような暗号化方式に用いる暗号鍵を持ち、通常、プログラムの一定領域に埋め込まれるかあるいはユーザには見えない部分あるいはファイルに秘匿されている。もちろん、暗号方式はこれ以外のものでもよい。簡易化する方法として、単に値の排他的論理和を取る方法等でもよい。また秘匿の方法もこれに限るものではない。

【 0 0 3 1 】

また、暗号化データ復号部 1 0 2、暗号化テーブル情報復号部 1 1 0、暗号化情報復号部 1 0 9 は同じものであっても構わないし、異なるものであってもよい。

【 0 0 3 2 】

なお、上記のステップに従ってプログラムをロードし、プログラムを実行した後メモリ空間上に展開されたプログラムは、実行直後に消去してもよいし、または次のプログラムがロードされる際に上書きすることによって消去するようにしてもよい。このようなプログラムを消去するタイミングは、そのプログラムの重要性やパフォーマンスによってプログラム生成時にユーザが別途指定するようにしてもよい。

【 0 0 3 3 】

次に、実施の形態 2 について述べる。

【 0 0 3 4 】

(実施の形態 2)

実施の形態 1 のメモリ配置情報保持部 1 0 4 は、プログラム生成時に決定された固定されたメモリ配置情報を保持しているため、上記プログラム実行時に各分割されたプログラムは毎回同じ配置位置にロードされる。この毎回同じ配置位置をハッカーによって見破られることを避けるために、プログラムロード領域指定部 1 1 2 によって、各分割プログラムをロードするメモリ領域を毎回変化させる。また、プログラム配置位置決定部 1 1 3 によって、このメモリ配置情報保持部 1 0 4 に保持するメモリ配置情報を毎回変化させる。

【 0 0 3 5 】

図 6 はメモリ配置情報保持部 1 0 4 が保持するメモリ配置情報の図である。

【 0 0 3 6 】

プログラム配置位置決定部 1 1 3 が決定するメモリ空間上の配置位置情報は、図 4 に示すようなメモリ配置位置情報および図 6 の (1) ～ (3) に示されるようにプログラムがロードされる度にアドレス情報が入れ替わる。

【 0 0 3 7 】

実施の形態 2 の動作の流れを実施の形態 1 の＜プログラムのロード手順＞を用いて説明する。＜プログラムのロード手順＞ 1 . ～ 9 . までは実施の形態 1 と同様である。

【 0 0 3 8 】

実施の形態 1 の＜プログラムのロード手順＞の 1 0 . 以降の代わりに以下のような手順で動作する。

【 0 0 3 9 】

1 0 . プログラムロード領域指定部 1 1 2 は、分割プログラムをロードするメモリ領域の開始アドレスとサイズを指定し、メモリ配置情報保持部 1 0 4 が記憶する。

【 0 0 4 0 】

1 1 . 9 . で認証に成功した場合、プログラム A を 1 0 . で指定したプログラムロード領域内にロードする。このときのロード位置は、プログラム配置位置決定部 1 1 3 によって決定される。

【 0 0 4 1 】

1 2 . 9 . で認証に失敗した場合、配置情報の復号化は行わずに、プログラムの処理を中断し（S 5 1 7）、制御部 1 0 6 は、メモリ空間上に復号されたデータがロードされている場合は消去する（S 5 1 8）。

【 0 0 4 2 】

1 3 . 制御部 1 0 6 は、プログラム A が呼び出す順に分割されたプログラム B ～プログラム I を 1 . ～ 1 2 . の手順を繰り返すことによりロードし、実行する。

【 0 0 4 3 】

図 7 は、プログラム配置位置決定部 1 1 3 における配置位置決定の流れを示すフローチャートである。

【 0 0 4 4 】

1 1 - 1 . アドレステーブル情報保持部 1 0 3 で保持している分割プログラムのロード領域の管理情報と、ロードされている分割プログラムの管理情報と、ロードしようとしている分割プログラムのサイズを比較して、十分な空き領域があるかどうか調べる（S 7 0 1）。十分な空き領域があれば、1 1 - 2 . の処理に進む。なければ、1 1 - 3 . の処理に進む。

【 0 0 4 5 】

1 1 - 2 . 空き領域に分割プログラムをロードする（S 7 0 2）。1 1 - 5 . に進む。

【 0 0 4 6 】

1 1 - 3 . アドレステーブル情報保持部 1 0 3 から、ロードされている分割プログラムのうち、最も古くからロードされているものを求め、それを削除する（S 7 0 4）。1 1 - 4 . に進む。

【 0 0 4 7 】

1 1 - 4 . 削除された分割プログラムの管理情報をアドレステーブル情報保持部 1 0 3 から削除する（S 7 0 5）。1 1 - 1 . に戻る。

【 0 0 4 8 】

1 1 - 5 . ロードした分割プログラムの開始位置、サイズ、プログラム識別子をアドレステーブル情報保持部 1 0 3 に図 6 のように記憶させる（S 7 0 3）。

終了する。

【0049】

このようにプログラム配置位置決定部113は、メモリ配置情報保持部104が保持する予め定められたアドレスの代わりに、プログラムが実行される度に分割プログラムの配置位置を決定することにより、分割されたプログラムが毎回同じアドレスにロードされないようにすることが可能になる。

【0050】

なお、11-3.において、次にロードする位置を最も古くからロードされているものの上にロードする代わりに、ランダムに位置を決定することにより、各分割プログラムの先頭アドレスをずらして、毎回同じアドレスにロードされないようにするとしてもよい。

【0051】

また、11-3. および11-4. において、最も古い分割プログラムを削除し、十分な空き領域が得られるまで11-1. から繰り返すとしたが、繰り返しを行わず、最も古い分割プログラムの先頭から連続した領域に新しい分割プログラムをロードしてもよい。このとき、2つ以上の分割プログラムが1度に削除されることもある。

【0052】

以上のように動作するプログラムを生成するプログラム生成部111の動作について述べる。

【0053】

通常、ソースコードやライブラリの集合から実行形式のプログラムを生成する際には、コンパイラを用いてソースコードをオブジェクトコードに変換する。さらに、リンカを用いて、これらのオブジェクトコードや標準のライブラリを組み合わせ、実行形式のプログラムが生成される。

【0054】

本実施の形態のプログラム生成部111は、プログラムを市販のコンパイラでコンパイルした結果得られるオブジェクトファイルに対して、オーバレイロードを行うために必要な情報を追加してオブジェクトファイルを変形する。さらに、

市販のリンカを用いて、これらの変形したオブジェクトファイル、ローダ機能を実現するライブラリ、標準のライブラリから実行形式のプログラムを生成する。プログラム生成部 1 1 1 に市販のコンパイラやリンカの機能を組み込んでもよい。

【 0 0 5 5 】

【発明の効果】

以上、説明したように本発明は、分割プログラムをロードする際のメモリ領域を毎回指定可能として、ロードする領域のメモリ位置を毎回変えることにより、命令コードがロードされるアドレスが変えることができる。また、分割プログラムロード時にロードする開始位置を毎回決定することを可能とすることにより、命令コードがロードされるアドレスが変えることができる。これらの結果、プログラムの動作を解析することが困難になり、安全性の高い耐タンパ化プログラムが提供できる。

【図面の簡単な説明】

【図 1】

暗号化データ復号装置の構成を示す機能ブロック図

【図 2】

制御部が配置するメモリ配置構成の概念図

【図 3】

メモリ配置情報保持部が保持する暗号化されたアドレス情報および復号化されたアドレス情報およびハードディスク上のイメージ図

【図 4】

メモリ配置情報保持部が保持するメモリ空間上の配置位置を示す概念図

【図 5】

ロード処理を表すフローチャート

【図 6】

メモリ配置情報保持部が保持するメモリ配置情報の図

【図 7】

プログラム配置位置決定部における配置位置決定の流れを示すフローチャート

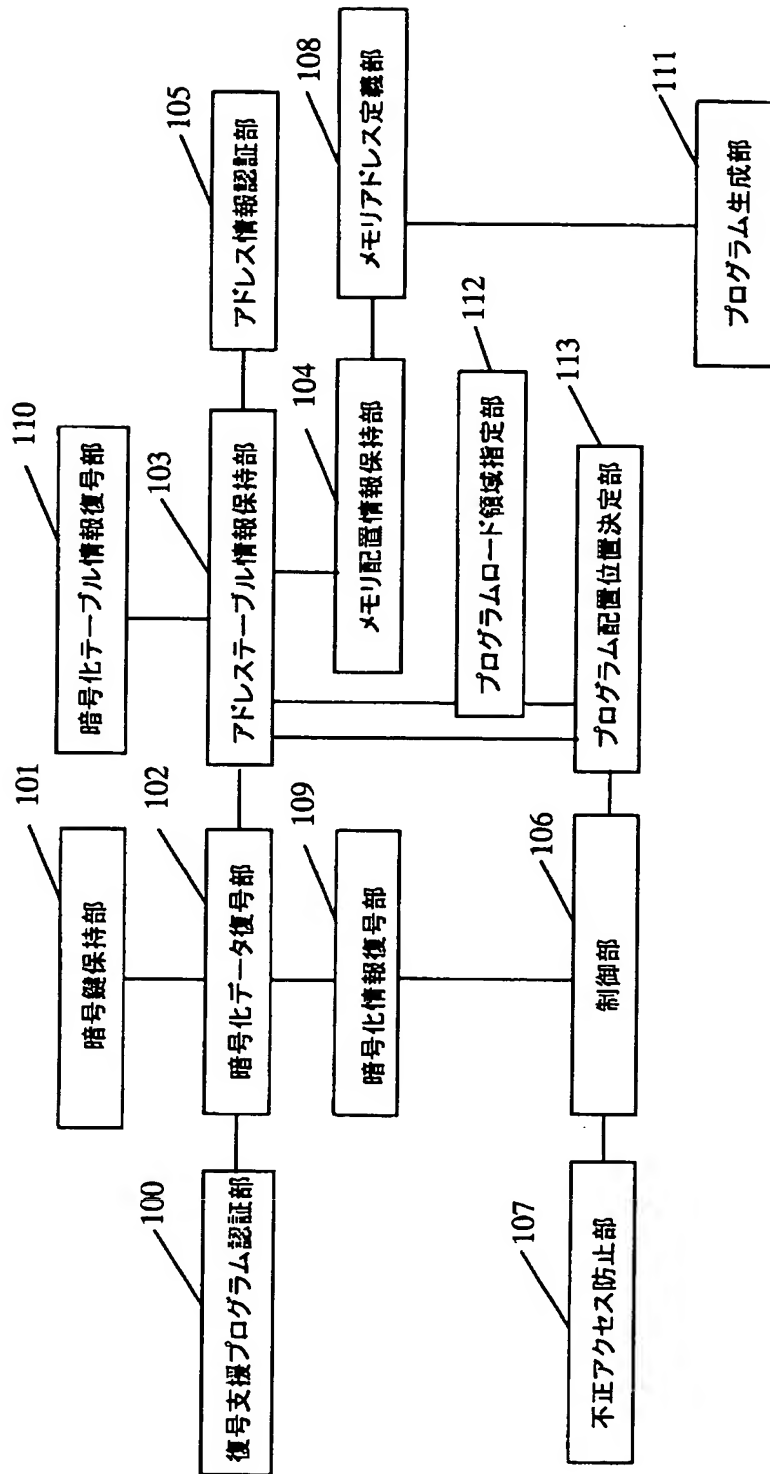
【符号の説明】

- 1 0 0 復号支援プログラム認証部
- 1 0 1 暗号鍵保持部
- 1 0 2 暗号化データ復号部
- 1 0 3 アドレステーブル情報保持部
- 1 0 4 メモリ配置情報保持部
- 1 0 5 アドレス情報認証部
- 1 0 6 制御部
- 1 0 7 不正アクセス防止部
- 1 0 8 メモリアドレス定義部
- 1 0 9 暗号化情報復号部
- 1 1 0 暗号化テーブル情報復号部
- 1 1 1 プログラム生成部
- 1 1 2 プログラムロード領域指定部
- 1 1 3 プログラム配置位置決定部

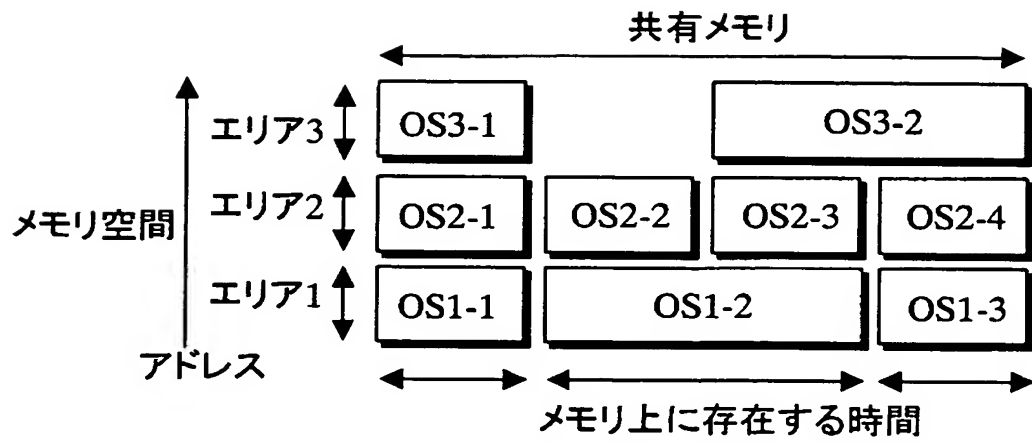
【書類名】

図面

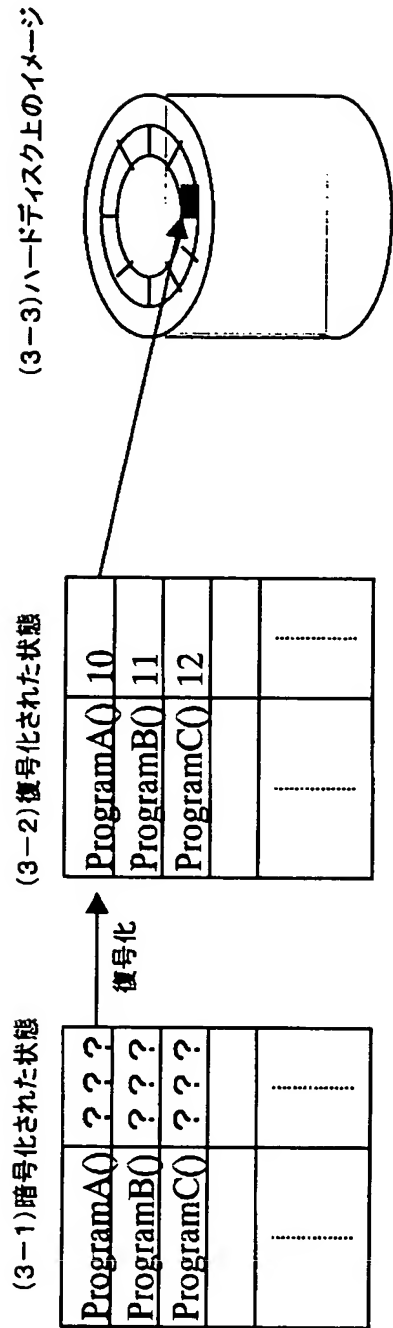
【図 1】



【図 2】



【図 3】



【図 4】

#Load data エリア 1-3

エリア 1 Program A= OS1-1

Program B= OS1-2

Program C= OS1-3

エリア 2 Program D= OS2-1

Program E= OS2-2

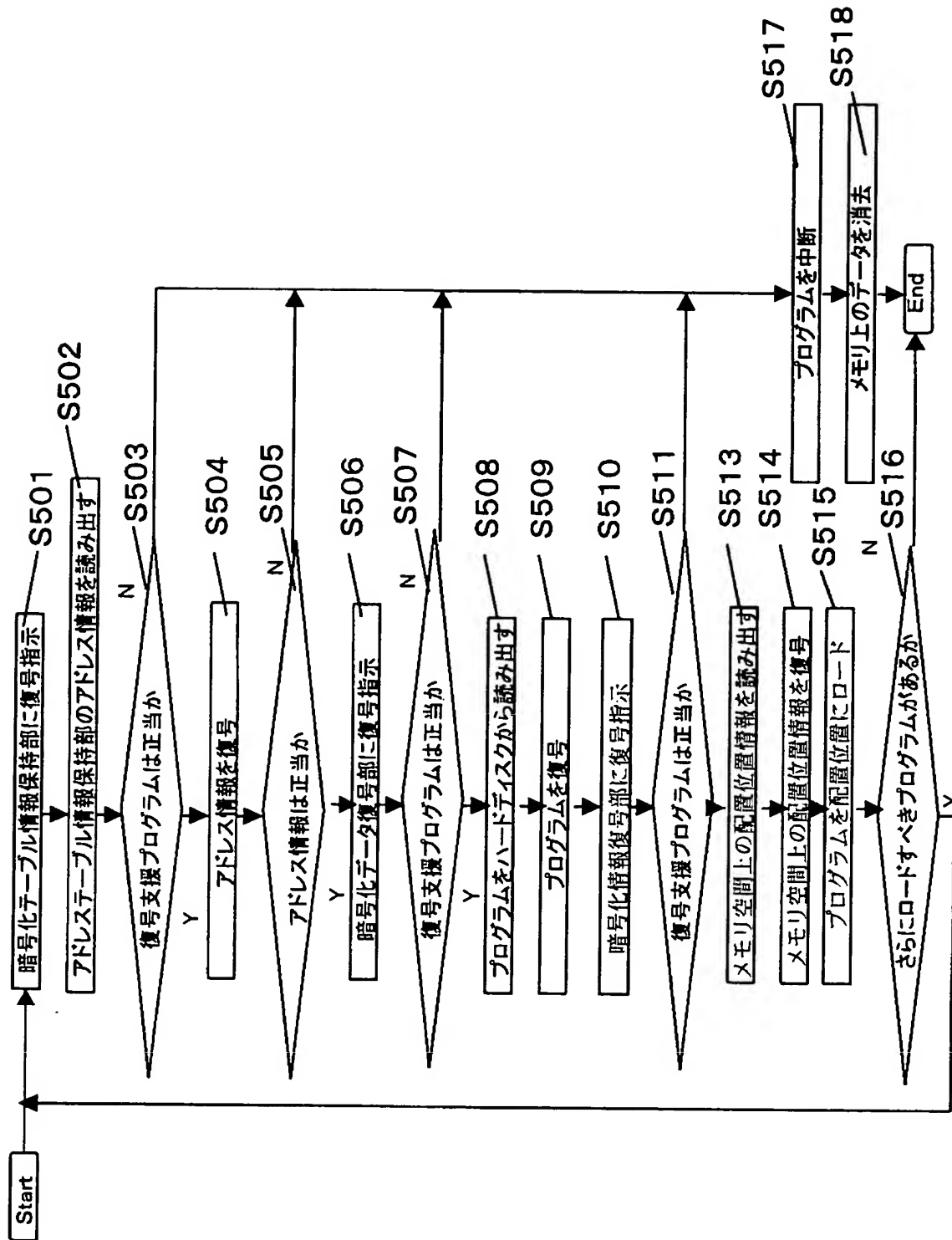
Program F= OS2-3

エリア 3 Program G= OS3-1

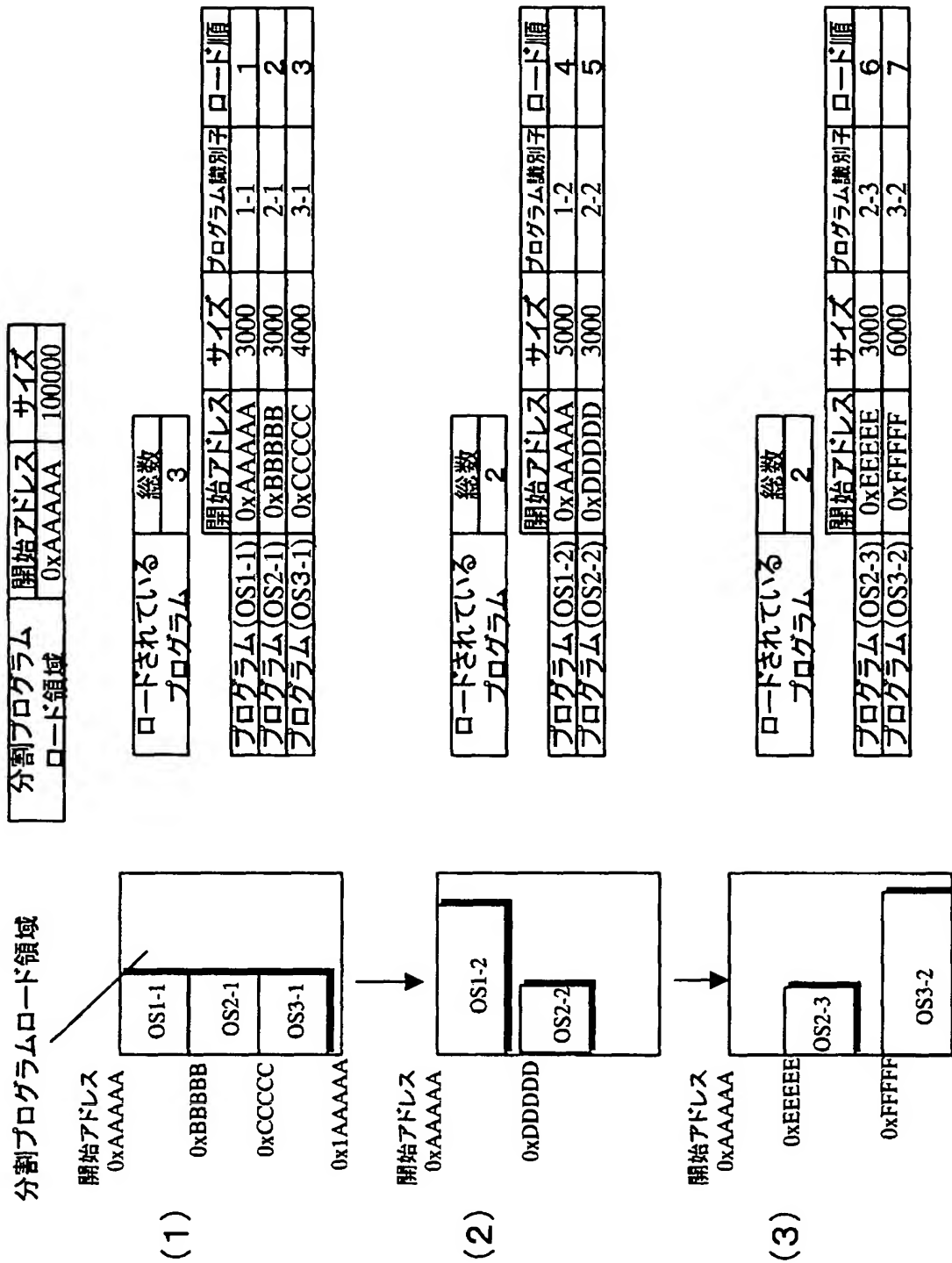
Program H= OS3-2

Program I = OS3-3

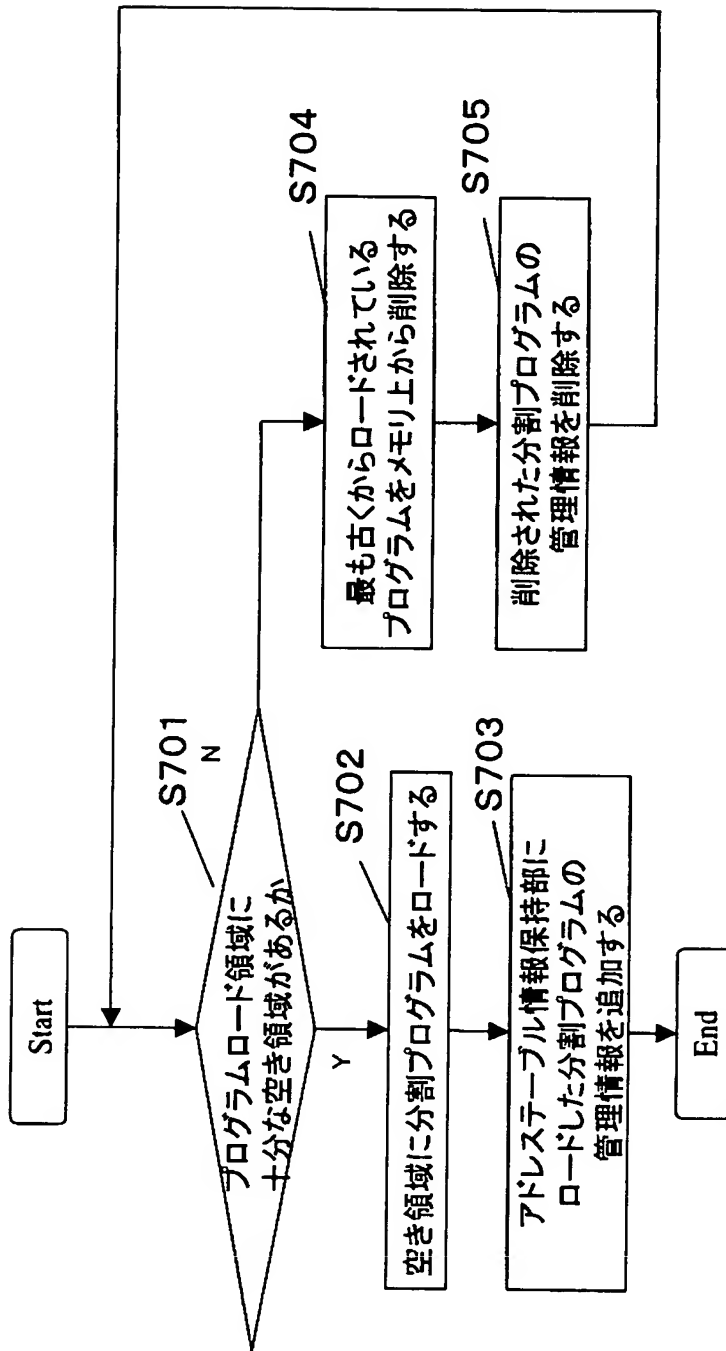
【図5】



【図 6】



【図 7】





【書類名】 要約書

【要約】

【課題】 分割プログラムをロードする領域のメモリ位置を毎回変えることにより、命令コードがロードされるアドレスを変えることができる耐タンパ化プログラムを提供する。

【解決手段】 単位毎に分割され暗号化されたプログラムをメモリ空間上にロードする際に、メモリ空間上の配置位置を保持するメモリ配置情報保持部と、プログラムの2次記憶装置上の位置情報を保持するアドレステーブル情報保持部と、分割され暗号化されたプログラムをメモリ空間にコピーし、ロードした位置、ロードしたプログラムのサイズ、識別子をアドレステーブル情報保持部に記憶させると同時に、すでに他のプログラムがロードされていた場合にはそのプログラムの管理情報をアドレステーブル情報保持部から削除するプログラム配置位置決定部とを有する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社